UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,214	08/22/2006	Pierre Girard	1032326-000405	6719

21839   7590   04/27/2009
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
TABOR, AMARE F

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
04/27/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/590,214
Filing Date: August 22, 2006
Appellant(s): GIRARD, PIERRE

Steven Ashburn
/Reg. No. 56,636/
<u>For Appellant</u>

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 02/26/2009 appealing from the Office

action mailed on 05/28/2008.

(1) Real Party Interest

A statement of identifying by name the real party interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

| 2003/0115457 A1 | Wildish et al. | 6-2003 |
| 2004/0123107 A1 | Miyazaki et al. | 6-2004 |

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

1.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description and enablement requirements. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

In a preliminary amendment to the claims and the specification filed on 08/22/2006, Applicant requested to insert the headings **Background of the Invention** (in page 1, line 4) and **Description of the Invention** (in page 6, between lines 13 and 14). The part of the disclosure that Applicant referred as Description of the Invention (starting from page 6, line 14 to page 11, line 25 of the disclosure) is a direct copy of the original claims 1 through 12 (see pages 12 to 16). This section does not describe the invention in detail description; however, it merely presents the claims as a summary of the invention.

Thus, the section can not be referred as Description of the Invention, but it could be referred as **Brief Summary of the Invention** (see item number (g) in the 2nd page of this office action). Therefore, if the heading **Description of the Invention** is inserted in page 10, between lines 25 and 26, only the two remaining paragraphs of the disclosure can be referred as Description of the Invention. The last two paragraphs (page 10, line 26 to page 11, line 25) describe two examples which are related to claims presented in claims 10-12. Since the section that Applicant referred as Description of the Invention is an

exact duplicate of the independent and dependent original claims listed from page 12 to 16, Examiner considers the disclosure of the invention as having only two parts: BACKGROUND OF THE INVENTION and CLAIMS (see items (f) and (j) above). In conclusion, the disclosure of the invention does not have sections that would support the claims in detailed explanation; i.e., it does not contain the two important parts of a specification (DETAILED DESCRIPTION and DRAWINGS, see item numbers (h & i) in the 2nd page of this office action), that would enable a person of skill in the art to understand the subject matter of Applicant's invention. Therefore, claimed invention presented in claims 1-20 clearly lacks the written description and enablement requirements.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9 and 13-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Wildish et al. (US 2003/0115457 A1, referred as "_Wildish_" hereinafter).

As per Claim 1, Wildish teaches,

A method of producing a digital certificate in which a certification authority performs the steps of grouping together, in a data set (see *abstract and Fig. 5*), a public key and digital data comprising data identifying the proprietor of the said public key and of an associated private key (see *ID1, ID2, ID3, Public key* in *Fig. 5*; and for example, *paragraph [0033]*), signing the data set in order to produce a digital certificate (see for example, *paragraphs [0004] & [0008]*), and storing the signed data set in a computer-readable storage medium (see *DATA 28* in *Fig. 5*), wherein the digital data also comprise data identifying at least one of means of generating the private key (see *KEY PAIR GENERATOR 27* in *Fig. 1*; and for example *paragraph [0008]*), means of storing the private key on a medium, and means of signing with the

private key (see *Fig. 4* and *DATA 28* and *CPU 20* in *Fig. 5; where keys are stored and signed;* and for example, *paragraph [0030]*).

As per Claim 8, Wildish teaches,

A digital certificate stored in a computer-readable medium (see *abstract and Fig. 5*), comprising: a public key (see *Public Key*), data identifying a proprietor of the public key and of an associated private key (see *ID1-ID3*), and data identifying at least one of means of generating the private key (see *KEY PAIR GENERATOR 27* in *Fig. 1*; and for example *paragraph [0008]*), means of storing the private key on a medium, and means of signature with said private key (see *DATA 28* and *CPU 20* in *Fig. 5; where keys are stored and signed*).

As per Claim 2, Wildish teaches,

in which the data identifying the means of generating the private key comprise data identifying: a method of generating the private key (see *paragraph [0008]*) and/or hardware on which the method of generating the private key is implemented, and/or a place on which the method of generating the private key is implemented (see *KEY PAIR GENERATOR* in *Fig. 5*).

As per Claim 3, Wildish teaches,

in which the data identifying the means of storing the private key comprise data identifying: a method of storing the private key on a medium (see *DATA 28* in *Fig. 5*), and/or hardware on which the method of storing the private key is implemented, and/or a place on which the method of storing the private key is implemented (see for example, *paragraphs [0011]-[0012] and [0033]*), and/or a storage medium on which the private key is stored (see *KEY PAIR GENERATOR* and *DATA 28* in *Fig. 5*).

Claim 13 is rejected for the same reasons applied to rejection of Claim 3.

As per Claim 4, Wildish teaches,

in which the data identifying the signature means comprise data identifying: a signature method using the private key (see *Fig. 2*), and/or a memory medium on which the said signature method is stored (see *DATA* in *Fig. 5;* for example, *paragraphs [0011]-[0012] and [0033]*).

Claims 14 and 15 are rejected for the same reasons applied to rejection of Claim 4.

As per Claim 5, Wildish teaches,

in which the data identifying hardware or a storage medium comprise: a reference identifying the said hardware or the said storage medium, and/or an identification of a manufacturer of the said hardware

or of the said storage medium (see *Fig. 3 & 4;* and for example, *paragraphs [0029] to [0031]*), and/or an indication of a security level of the said hardware or of the said storage medium defined according to a standard ISO 15408 (see *paragraphs [0005] & [0011]; where security protocols are disclosed*).

Claims 16 and 17 are rejected for the same reasons applied to rejection of Claim 5.

As per Claim 6, Wildish teaches,

in which the data identifying a method comprise: a reference identifying the said method of generating the private key (see *abstract; Fig. 2;* and for example, *paragraphs [0008], [0010], [0012], [0019]-[0020], [0026] & [0031]-[0032]*), and/or an identification of an inventor of the said method of generating the private key(see *RANDOM NUMBER GENERATO 26* in *Fig. 5*), and/or an indication of a security level of the said method of generating the private key according to ISO 15408 (see *paragraphs [0005] & [0011]; where security protocols are disclosed*).

Claims 18-20 are rejected for the same reasons applied to rejection of Claim 6.

As per Claim 7, Wildish teaches,

in which the data identifying a place comprise: an identification of the said place, and/or an identification of a security level of the said place according to ISO 15408 (see *paragraphs [0005] & [0011]; where security protocols are disclosed*).

As per Claim 9, Wildish teaches,

of the X509 type according to a standard Information Technology - Open Systems Interconnection - The Directory : Public Key and Attribute Certificate Frameworks, dated March 2000, of the International Telecommunication Union, in which a set of predefined free fields are used to store the digital data identifying (see *Fig. 1;* and for example, *paragraphs [0005] and [0019]*): a method of generating the private key, and/or hardware on which the method of generating the private key is implemented, and/or a place on which the method of generating the private key is implemented (see *KEY PAIR GENERATOR 27* in *Fig. 5*), and/or a method of storing the private key on a medium, and/or hardware on which the method of storing the private key is implemented (see *KEY PAIR GENERATOR* in *Fig. 5*),

and/or a place on which the method of storing the private key is implemented, and/or a storage medium on which the private key is stored (see *DATA 28* in *Fig. 5*), and/or a signature method using the private key (see for example, *paragraphs [0011]-[0012] and [0033]*), and/or a storage medium on which the said signature method is stored (see *DATA* in *Fig. 5;* for example, *paragraphs [0008],[0012] and [0030]*).

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

**Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over _Wildish_ in view of
"Miyazaki" et al. (US 2004/0123107 A1, referred as "_Miyazaki_" hereinafter).**

As per Claims 10-12, Wildish teaches,

receiving a message signed with a private key (see *the packet switched network* in *Fig. 3*),
reading, in the digital certificate, data identifying means of generating the private key (see *Fig.* 2) and/or
means of storing the private key on a medium and/or means of signing with the private key (see *Fig.* 5).

Wildish fails to teach deducing therefrom a probability of the said private key having been used by
a legitimate proprietor of the said private key, according to the said probability, accepting or refusing the
electronic message; in which the message is accepted solely if the probability of the said key having been
used by its legitimate proprietor is greater than a predefined value; and in which: the message is
accepted if the probability is greater than a first value (VB1), a confirmation of the said message is
requested if the probability is between the first value (VB1) and a second value (VB2) less than the first
value, and the message is refused if the probability is less than the second value (VB2).

However, in the same field of endeavor Miyazaki teaches message is accepted solely if the
probability of the said key having been used by its legitimate proprietor is greater than a predefined value
(see *paragraphs [0121]-[0122], [0126] and [0135]-[0136]*).

It would have been obvious to a person having ordinary skill in the art at the time of Applicant's
invention to combine the teachings of Miyazaki and the system of Wildish because both inventions are
directed to method of securing digital networks using digital signature. One having ordinary skill in the art
would be motivated to incorporate the teachings of Miyazaki in order to decide whether to accept or reject
a message and verify the reliability of the signature history (see *abstract* and *paragraph [0008]* of
Miyazaki).

(10) Response to Argument

(A) Rejection of Claims 1-20 under 35 U.S.C. 112, 1st paragraph

Appellant argued: "*Appellant respectfully submits one of ordinary skill in the art would have sufficient knowledge to make and use the claimed invention based on the "Detailed Description" section between page 6, line 14 and page 11, line 25 of Appellant's specification.*"

Examiner disagrees with appellant's argument.

Examiner notes that, the section appellant identified as '**Detailed Description**' [*page. 6, line 14 to page. 11, line 25*] is merely copy of the original claims. Except the first paragraph [*used as an introduction*] and the last paragraphs [*15-17, which describe two examples related to claims 10-12*], the major portion of the '**Detail Description**' [*paragraphs 2 to 14*] is copy of the original Claims 1-12.

For the convenience of the Board, examiner has summarized the <u>**ENTIRE SPECIFICATION**</u> of the invention [*from the first page, page.1 to the last page, page.16 of original disclosure*] in the following table.

Please note that the invention is disclosed as:

(i) <u>**Background of the Invention**</u> – (page.1, line 5 through page.6, line 13);

(ii) <u>**Detail Description of the Invention**</u>- (page.6, line 14 through page.11, line 25); and

(ii) <u>**Claims**</u> – (pages 12-16).

METHOD OF PRODUCING A DIGITAL CERTIFICATE, THE ASSOCIATED DIGITAL CERTIFICATE, AND A METHOD OF USING SUCH A DIGITAL CERTIFICATE

Background of the Invention [page 1, line 5 to page 6, line 13]

Detail Description of the Invention [page 6, line 15 to page 11, line 25]		**Claims** [pages 12-16]	
	Paragraph		*Claim(s)*
1	The aim of the invention is to resolve this problem by proposing a method …		--
2 & 3	For this the invention proposes a method of producing a digital certificate during which a certification authority…means of signing with the private key.	1	A method of producing a digital certificate during which a certification authority….means of signing with the private key.
4	The data identifying the means of generating the private …generating the private key is implemented.	2	A method according to claim 1, in which the data identifying means of generating the private… generating the private key is implemented.
5	The data identifying means of storing the private key…on which the private key is stored.	3	A method according to claim 1 or 2, in which the data identifying means of storing the private key…on which the private key is stored.
6	Finally, the data identify …method is stored.	4	…the data identify…method is stored.
7	The data identifying hardware or a storage …standard ISO 15408 dated 1.12.99	5	…data identifying hardware or a storage…standard ISO 15408.
8	The data identify…according to ISO 15408.	6	…the data identify…according to ISO 15408.
9	The data identify…according to ISO 15408.	7	…the data identify…according to ISO 15408.
10	The invention also concerns a digital certificate comprising: a public key, a data identifying…said private key.	8	A digital certificate comprising: a public key, a data identifying…said private key.
11	In preferred embodiment this certificate is of X509 type according to…method is stored.	9	A certificate according to claim 8, of the X509 type according to…method is stored.
12	The invention also concerns a method of using a digital certificate…said private key.	10	A method of using digital certificate…of said private key.
13	It is possible for example to choose …greater that predefined value.	11	…message is accepted solely if…greater that a predefined value.
14	It is also possible to choose to: accept the message…is less than the second value.	12	A method…the message is accepted if… is less than the second value (VB2).
15-17	To estimate the probability of the private key…is used [**paragraph 15**]. In one example, the information present … that he has received [**paragraph 16**]. In another example, the information present … in order to avoid any risk [**paragraph 17**].		The paragraphs describe two examples related to dependent **claims 10-12**
--	--	13-20	**New Claims** added in the preliminary amendment filed on 08/22/2006.

Therefore, examiner asserts that the disclosure of the invention **does not** describe in detail

[*either in writing, or in example(s) and/or in figure(s)*] the claims presented for examination. Thus, one of

ordinary skill in the art would not have sufficient knowledge to make and use the claimed invention.

(B) Rejection of Claims under 35 U.S.C. 102(e) as being anticipated by "Wildish"

Claims 1 and 8

Appellant argues that, "*Wildish cannot support a rejection of claim 1 under Section 102(e) because the document fails to teach, at least, "digital data comprising data identifying at least one of: means of generating the private key, means of storing the private key on a medium, and means of signing with the private key.*"

Examiner respectfully disagrees with appellant's argument, because examiner asserts that the claimed features of Claims 1 and 8 are anticipated by **Wildish**. Specifically, examiner notes that, **Wildish** discloses *"digital data comprising data identifying at <u>**least one of**</u>: <u>means of generating the private key</u>, means of storing the private key on a medium, and means of signing with the private key*" because **Wildish** explicitly discloses the claimed feature "*means of generating the private key.*" For example, **Wildish** discloses that [par.0030, lines 1-2], "*[T]he root server 14 generates a private/public key pair in a conventional manner.*" In other words, **Wildish** clearly discloses <u>the root server 14</u> as a '*means for generating the private key.*'

Additionally, examiner notes that, **Wildish** also discloses the claimed feature *"means of signing with the private key"*. For example, **Wildish** discloses that [par.0030, lines 2-7], "*[T]he root server 14 then issues a digital certificate certifying the public key or a next level subordinate server 16 or end user 12. <u>This digital certificate is signed by its private key</u> so that ...*"

Claims 2-7, 9 and 10-20

Appellant argues that, Claims 2-7, 9 and 10-20 are dependent claims, depending from distinguishable independent claims.

Examiner would point out that, arguments with respect to the independent claims have been traversed as indicated above; and therefore, arguments with respect to claims 2-7, 9 and 10-20 are traversed with the same rationale thereto.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Amare Tabor/

Examiner, Art Unit 2434

Conferees:

Andrew Nalven

/Andrew L Nalven/

Primary Examiner, Art Unit 2434

Kambiz Zand

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434